SYSTEM AND METHOD FOR DATA ACCESS AND CONTROL

FIELD OF THE INVENTION

[0001] The present invention relates generally to a process for controlling and providing access to secured electronic data and more particularly to a multilevel security process for processing requests and determining user authorization to access both secured electronic data and the means for accessing the secured electronic data.

BACKGROUND OF THE INVENTION

[0002] The benefits of securing data from unauthorized access are well known. However, many data security techniques are cumbersome in that they are fraught with parallel paths, circuitous routings, delays and frequent mistakes. Accordingly, an improved method for providing access to secured data would be advantageous.

SUMMARY OF THE INVENTION

[0003] The present invention mitigates or solves the above-identified limitations in known solutions, as well as other unspecified deficiencies in known solutions. A number of advantages associated with the present invention are readily evident to those skilled in the art, including economy of design and resources, transparent operation, cost savings, etc.

[0004] In accordance with one embodiment of the present invention, a method for providing an access candidate access to secured electronic data is disclosed. The method comprises the steps of submitting a request for access candidate access to the secured electronic data to a controller associated with the secured electronic data, comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data, submitting, by the controller, a request for authorization to a resolution authority when the comparison indicates that access by the access candidate is prohibited without authorization, and granting the access candidate access to the secured electronic data when the resolution authority provides authorization for such access.

[0005] In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing access to the electronic data by the one or more resources, a method for providing an access candidate access to the electronic data is disclosed in accordance with another embodiment of the present

invention. The method comprises the steps of submitting a request for access to the first security level, granting the access candidate access to the first security level when a comparison of one or more attributes of the access candidate with one or more access requirements associated with the first security level indicates that access to the first security level by the access candidate is not prohibited and submitting a request for access to the second security level. The method further comprises the steps of submitting a request for authorization to a resolution authority when a comparison of one or more attributes of the access candidate with one or more access requirements associated with the second security level indicates that access to the second security level by the access candidate is prohibited without authorization and granting the access candidate access to the second security level should the resolution authority provide authorization.

[0006] In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing the electronic data, a method for providing an access candidate access to the electronic data is provided in accordance with an additional embodiment of the present invention. The method comprises the steps of identifying a plurality of data subsets of the electronic data, determining, for each data subset, at least one data class associated with the data subset, the at least one data class identifying at least a citizenship requirement and a location requirement for access to data associated with the data class and submitting, by a first sponsor of the access candidate, a request for access to the first security level, the request including an indication of a citizenship status of the access candidate, an indication of a current location of the access candidate, and an indication of an existence of a data access agreement with the access candidate. The method further comprises the steps of granting the access candidate access to the first security level based at least in part on an evaluation of the request for access to the first level, submitting, by a second sponsor of the access candidate, a request for access to at least one data subset at the second security level when access to the first security level has been granted, the request for access to the at least one data subset including an indication of a citizenship status of the access candidate and an indication of a current location of the access candidate, submitting a request for authorization to a resolution authority when a comparison of the citizenship status and the current location of the access candidate with the respective citizenship requirement and location

requirement of the at least one data class of the requested data subset indicates that access to a requested data subset at the second level by the access candidate is prohibited without authorization, and granting the access candidate access to the requested at least one data subset at the second security level when the resolution authority provides authorization upon receipt of the request for authorization.

[0007] In accordance with yet another embodiment of the present invention, a system for providing an access candidate access to secured electronic data is disclosed. The system comprises storage adapted to receive and store the electronic data, one or more resources adapted to access and manipulate the electronic data, and means for evaluating a request for access candidate access to the one or more resources the evaluation of the request including a first comparison of one or more attributes of the access candidate with one or more access requirements associated with the one or more resources. The system further comprises means for granting the access candidate access to the one or more resources when the first comparison indicates that access is not prohibited and means for evaluating a request for access candidate access to the electronic data by the one or more resources, the evaluation of the request including a second comparison of one or more attributes of the access candidate with one or more access requirements associated with the electronic data. The system additionally comprises means for submitting a request for authorization to a resolution authority when the second comparison indicates that access to the electronic data by the access candidate is prohibited without authorization and means for granting the access candidate access to the electronic data using the one or more resources when the resolution authority provides authorization.

[0008] In accordance with an additional embodiment of the present invention, a system for providing an access candidate access to secured electronic data is provided, the electronic data being associated with one or more data classes, each data class identifying at least a citizenship requirement and a location requirement for access to data associated with the data class. The system comprises storage adapted to receive and store the electronic data, one or more resources adapted to process and manipulate the electronic data, and a resource access controller adapted to grant access to the one or more resources based at least in part on a comparison of a citizenship status and a current location of the access candidate and an existence of a data access agreement with a citizenship requirement, location requirement and data access

agreement requirement associated with the one or more resources. The system further comprises one or more data access controllers adapted to grant access to a corresponding portion of the electronic data based at least in part on a comparison of a citizenship status and a current location of the access candidate with a citizenship requirement and a location requirement associated with one or more data classes of the corresponding portion of the electronic data and one or more resolution authorities adapted to authorize access to one or more portions of the electronic data when a comparison performed by a corresponding data access controller indicates access is prohibited without authorization. The system additionally comprises a data access module adapted to evaluate a request for access to one or more portions of the electronic data by the one or more resources to identify one or more data access controllers corresponding to the one or more portions of the electronic data and forward the request for access to the one or more identified data access controllers for evaluation as to whether to grant the access candidate access to the corresponding one or more portions of the electronic data.

[0009] In accordance with yet another embodiment of the present invention, a method for determining an access candidate's access to secured electronic data is provided. The method comprises the steps of submitting a request for access to the secured electronic data to a controller associated with the secured electronic data, comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the secured electronic data, and submitting, by the controller, a request for authorization to a resolution authority when the comparison indicates that access by the access candidate is prohibited without authorization, wherein the resolution authority processes access candidate information, requests related information and determines whether to authorize the access candidate's access to the secured electronic data. The method further comprises granting or denying by the controller, in whole or in part, the access candidate access to the secured electronic data based at least in part on the resolution authority's determination.

[0010] In accordance with an additional embodiment of the present invention, a method for determining an access candidate's access to secured electronic data is provided. The method comprises the steps of submitting a request for access to the secured electronic data to a controller associated with the secured electronic data, comparing, at the controller, one or more attributes of the access candidate with one or more access requirements associated with the

secured electronic data, and granting the access candidate access to the secured electronic data when the comparison indicates that access by the access candidate is not prohibited. The method further comprises the steps of submitting, by the controller, a request for authorization to a resolution authority when the comparison indicates that access by the access candidate is prohibited without authorization and performing the following steps: the resolution authority processing access candidate information and request related information and determining whether to authorize the access candidate's access to the secured electronic data; and granting or denying by the controller, in whole or in part, the access candidate access to the secured electronic data based at least in part on the resolution authority's determination.

[0011] In a data security system having a first security level securing one or more resources for manipulating electronic data and a second security level securing access to the electronic data by the one or more resources, a method for determining an access candidate's access to the electronic data is provided in accordance with yet another embodiment of the present invention. The method comprises the steps of submitting a request for access to the first security level, determining the access candidate's access to the first security level based on a comparison of one or more attributes of the access candidate with one or more access requirements associated with the first security level, submitting a request for access to the second security level, submitting a request for authorization to a resolution authority when a comparison of one or more attributes of the access candidate with one or more access requirements associated with the second security level indicates that access to the second security level by the access candidate is prohibited without authorization and determining by the resolution authority the access candidate's access to the second security level.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] The purpose and advantages of the present invention will be apparent to those of ordinary skill in the art from the following detailed description in conjunction with the appended drawings in which like reference characters are used to indicate like elements, and in which:

[0013] Figure 1 is a schematic diagram illustrating an exemplary multilevel data access system in accordance with at least one embodiment of the present invention.

[0014] Figure 2 is a flow diagram illustrating an exemplary process for providing access to resources used to manipulate secured data in accordance with at least one embodiment of the present invention.

[0015] Figure 3 is a flow diagram illustrating an exemplary process for accessing secured data using the resources of Figure 2 in accordance with at least one embodiment of the present invention.

[0016] Figure 4 is a block diagram illustrating an exemplary implementation of an access profile as part of a graphical display in accordance with at least one embodiment of the present invention.

[0017] Figure 5 is a table illustrating exemplary access attributes associated with various exemplary data classes in accordance with at least one embodiment of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

[0018] The following description is intended to convey a thorough understanding of the present invention by providing a number of specific embodiments and details involving access to secured electronic data. It is understood, however, that the present invention is not limited to these specific embodiments and details, which are exemplary only. It is further understood that one possessing ordinary skill in the art, in light of known systems and methods, would appreciate the use of the invention for its intended purposes and benefits in any number of alternative embodiments, depending upon specific design and other needs.

[0019] Figures 1-5 illustrate exemplary techniques for providing access to secured electronic data. In at least one embodiment, an access candidate gains access to some or all of the secured data by gaining access to two sequential levels of security, where the first security level secures access to the resources used to manipulate the secured data and the second security level secures access to the secured data by the resources. To gain access to the resources, a sponsor of the access candidate submits an access request. Access attributes associated with the access candidate are considered in deciding whether to grant or deny access to the resources. After access to the resources is obtained, the same sponsor or a different sponsor submits a request for access to one or more portions of the secured data. Based on a comparison of one or more access requirements of the one or more portions of the secured data with the applicable access attributes of the access candidate, a decision on whether to grant access to the requested

portions of the secured data is made. If access is granted (or not prohibited), the access candidate may use the resources to manipulate the secured data. If access is prohibited without authorization, a resolution request may be submitted to a resolution authority. The resolution authority may use the attributes, the access requirements as well as additional information to decide whether to authorize the grant of access or decline authorization. As used herein, the term access candidate preferably includes an entity requiring or desiring access to some or all of the secured data, such as a newly hired employee assigned to a project having secured data. The data may be discrete elements of data, collections of data or data files, an entire or portion of a database, etc.

[0020] Referring now to Figure 1, an exemplary multilevel data access system 100 is illustrated in accordance with at least one embodiment of the present invention. The system 100 preferably is utilized to provide authorized users access to secured electronic data 102 while preventing access by unauthorized users. The electronic data 102 may be secured using any of a variety of techniques known to those skilled in the art. For example, the electronic data 102 may be stored in one or more databases or files that are protected by password, access permissions, and/or encryption. Further, the electronic data 102 may be stored in one or more directories having security measures in place, such as hidden directories, password or encryption protected directories, and the like. As discussed in greater detail below, the electronic data 102 further may be secured from access by securing the resources used to manipulate the electronic data 102. For example, the data may be manipulated in any of a variety of data operations, such as, for example, displaying data, copying data, transferring data, deleting data, modifying data, printing data, and the like. The data access system of the present invention may be employed in a number of systems, including, for example, a knowledge management system.

[0021] The system 100, in at least one exemplary embodiment, includes two security levels: a mandatory access control (MAC) security level 104 and a discretionary access control (DAC) security level 106. To gain access to secured electronic data, an access candidate 108 preferably must successfully access both the MAC security level 104 and the DAC security level 106.

[0022] The MAC security level 104 preferably is configured to control access to one or more resources 110 used to manipulate the secured data. The resources 110 may include, for

example, a computer or processor based workstation and related software connected to a secured data server storing the secured data 102, a software application used to manipulate the secured data 102, a printer used to provide a printed representation of the secured data 102, etc. To illustrate, in one embodiment, the MAC security level 104 may be implemented in part as the security checkpoint through which the access candidate 108 gains physical access to the workstation and software applications (i.e., resources 110) used to access the secured data. Physical access to the resources 110 may be accomplished by, for example, gaining access to a facility housing the resources 110. Physical access may also include logging on to the workstation or software application used to access secured data.

[0023] After gaining physical access, the MAC security level 104, in one embodiment, also is responsible for granting directory access. Directory access preferably includes access to basic network resources, such as accounts provided for email access, access to the access candidate's home drive, access to public directories, etc. Directory access preferably provides access to less sensitive data and applications typically found, for example, on Internet portals. For example, the resources 110 may include a website used to display secured data and the MAC security level 104 may be implemented as a security protocol through which the access candidate 108 gains directory access to the website.

[0024] The MAC security level 104 may grant access to the access candidate 108 in any of a variety of ways. Preferably, the MAC sponsor 112 submits an access request 114 as an indication that the MAC sponsor 112 desires to have MAC access granted to the access candidate 108. However, the access request 114 may be submitted by the access candidate 108, the MAC sponsor 112, or a combination thereof. The MAC sponsor 112 may be associated with the access candidate 108 in any of a variety of ways. For example, the MAC sponsor 112 may include an employer or supervisor or business associate of the access candidate 108, an "owner" or controller of part or all of the secured data 102 or resources 110, a neutral third party, and the like. Although illustrated in the figures in human form, "sponsors" may be in the form of automated processes and may or may not involve human interaction.

[0025] Additionally, an access profile 116A associated with the access candidate preferably is submitted for evaluation. The access profile 116A may be submitted by the access candidate 108, the MAC sponsor 112, or a combination thereof. Alternatively, the access profile

116A may be retrieved for review from, for example, network or third party storage. The access profile 116A includes one or more access attributes associated with the access candidate 108 that may be useful to the MAC security level 104 in deciding to grant or deny the access request 114 submitted by the MAC sponsor 112. The attributes typically are specific to the requirements necessary to access the resources 110 via the MAC security level 104. For example, in certain circumstances, access to the resources 110 may be predicated on the existence of a valid data access agreement (e.g., an agreement not to disclose information without prior authorization) with the access candidate 108, that the access candidate 108 have a certain citizenship status and that the access candidate 108 is located within a certain geographical or political boundary. In such circumstances, the access profile 116A may include an indication of the existence of a data access agreement and an indication of the access candidate's citizenship and current location, among other applicable attributes. Documents and other evidence may be submitted by the access candidate 108 or MAC sponsor 112 to verify the information provided in the access profile 116A.

[0026] The comparison of the access profile 116A with the access attributes required for the grant of access to resources 110 may be performed manually, such as by a security technician who reviews the request 114, the access profile 116A and any supplied proof against the access attributes. Alternatively, the comparison may be automated, in whole or in part, by an automated system (e.g., a software application) adapted to review the request 114, the access profile 116A and any supplied proof.

[0027] Should the comparison indicate that access is prohibited without authorization, the MAC security level 104 may so inform the MAC sponsor 112 and/or the access candidate 108. In the event that the access profile 116A incorrectly describes one or more attributes of the access candidate 108 and these errors were the cause of the denial of access, the MAC sponsor 112 or the access candidate 108 may correct the access profile 116A and resubmit the access profile 116A for reconsideration. If, however, the attributes of the access candidate 108 were described correctly, the MAC sponsor 112 and/or the access candidate 108 may attempt to change one or more attributes (e.g., relocate the access candidate 108) or the MAC sponsor 112/access candidate 108 may appeal for a waiver of one or more access requirements or a modification of the access requirements.

[0028] Should the comparison indicate that the access candidate 108 is not prohibited from accessing the resources 110, the MAC security level 104 may grant the access candidate 108 access to the resources 110. Any of a variety of techniques may be used to grant access. For example, the access candidate 108 may be supplied one or a series of user identifications (ID) and/or passwords which may be used to access the resources 110 and/or a network profile associated with the access candidate 108 may be modified to allow access to the resources 110. Further, one or more administrators may modify access permissions associated with the access candidate's account. Access also may be granted by, for example, allowing the access candidate 108 to have physical access to the resources 110.

[0029] After gaining access to the resources 110, in one embodiment, the access candidate 108 is required to gain access to the secured data 102 via the DAC security level 106. In one embodiment, various portions of the secured data 102 are associated with one or more data classes, where each data class has a specific set of access requirements. For example, data may be separated into various data classes based on its ownership or origin. To illustrate, portions of the secured data 102 may include data provided by, or generated in cooperation with, a government entity, such as the Department of Energy (DOE), Department of Defense (DOD) or National Security Agency (NSA). Alternatively, although portions of the secured data 102 may not be classified per se, they may fall under one or more rules, regulations or laws controlling the transfer of sensitive information, such as laws and regulations applicable to the export of technical information. Accordingly, each of these providers or regulators of data may have various requirements for gaining access to the data, such as citizenship, current location, and the like. Accordingly, portions of the secured data 102 may be identified by data owner or originator, or by the laws, rules and regulations applicable to the data portions.

[0030] Access through the DAC security level 106 may be granted by submitting an access request 118 from a DAC sponsor 120 on behalf of the access candidate 108. As with the MAC sponsor 112, the DAC sponsor 120 may be associated with the access candidate 108 in any of a variety of ways. For example, the DAC sponsor 120 may be an employer or supervisor of the access candidate 108, an owner or manager of part or all of the secured data 102, or a neutral third party. In one embodiment, the MAC sponsor 112 and the DAC sponsor 120 are the same entity.

[0031] In addition to the access request 118, an access profile 116B associated with the access candidate 108 may be provided to, or obtained by, the DAC security level 106. The access profile 116B includes one or more attributes associated with the access candidate 108 that may be useful to the DAC security level 106 in deciding to grant or deny the access request 118 submitted by the MAC sponsor 120. As noted above, various data classes may be associated with the secured data, where each data class has a specific set of access requirements. Accordingly, the access profile 116B may include attributes related to the access requirements of the data classes to which the secured data 102, or requested portion(s) thereof, belongs. The access requirements may include, for example, a certain citizenship status, a certain current geographical location, the existence of a valid data access agreement with the access candidate 108, and the like. In at least one embodiment, the access profile 116A and the access profile 116B are the same access profile. Further, as described in greater detail below with reference to Figure 4, the access profiles 116A, 116B preferably are implemented as part of a graphical display.

[0032] The DAC security level 106 may be adapted to compare the access profile 116B with the access attributes associated with the one or more data classes of the requested portion(s) of the secured data 102. The comparison may be performed manually or the comparison may be automated, in whole or in part, by an automated system adapted to review the request 118, the access profile 116B and any supplied proof.

[0033] Should the comparison performed by the DAC security level 106 indicate that access to one or more data classes of the secured data is prohibited without authorization, the DAC security level 106 may submit a resolution request 122 to a resolution authority 124. The resolution authority 124, in one embodiment, includes an entity or automated system authorized to provide authorization for access, such as, for example, an "owner" of the data, a supplier of the data, and the like. The authorization may be determined by granting a waiver of the access requirements of one or more data classes, modifying the access requirements, excluding data assigned to one or more prohibited data classes from access by the access candidate 108, and the like. In the event that authorization cannot be resolved based on the supplied request, the DAC security level 106 may so inform the DAC sponsor 120 and/or the access candidate 108. The

DAC sponsor 120 and/or access candidate 108 then may attempt to change one or more attributes associated with the access candidate 108 and resubmit the access request 118.

[0034] Should the comparison indicate that the access candidate 108 is not prohibited from accessing the secured data 102 or should the resolution authority 124 provide authorization, the DAC security level 106 may grant the access candidate 108 access to the portion(s) of the secured data 102 for which access is sought. Any of a variety of techniques may be used to grant access including, for example, the provision of a password, the modification of a network profile, or the transfer of secured data from a secure storage location to a location accessible by the resources 110. After access is granted by the DAC security level 106, the access candidate 108 may utilize the resources 110, as well as additional resources, to manipulate and modify the requested portion of the secured data.

[0035] In at least one embodiment, various portions of the secured data 102 are associated with one or more levels of data. For example, the secured data 102 may be grouped into an application level 126, a group information level 128 and an item information level 130. The application level 126 may include, for example, one or more software applications (e.g., application 132) that are enabled to create and modify data 134, where the data 134 may be an integral portion of the application or may be disassociated from the application 132. The group information level 128 may include, for example, a hierarchical collection of data (e.g., data 136-140) that may or may not be associated with a specific software application. The item information level 130 may include, for example, low level data (e.g., data 142) that may or may not be associated with a specific software application. Accordingly, the above-described process for accessing a portion of the secured data 102 via the DAC security level 106 preferably is repeated for each level to which the portion of secured data 102 belongs. To illustrate, if the access candidate 108 desires access to a portion of the secured data 102 that is a member of both the group information level 128 and the item information level 130, the DAC security level access process may be performed twice, once for the group information level 128 and once for the item information level 130, before the access candidate 108 may access the data.

[0036] Referring now to Figure 2, an exemplary network-based MAC access process 200 is illustrated in accordance with at least one embodiment of the present invention. As noted above, a grant of access by the MAC security level 104 (Figure 1) preferably is required before

an access candidate 108 may access the resources 110 used to manipulate the secured data 102. In at least one embodiment, the process for granting MAC access is performed at least in part through the use of a network 202, where the network 202 may include the Internet, a local area network (LAN), a wide area network (WAN), and the like.

[0037] The network 202 preferably is used to connect a workstation 204 used by the MAC sponsor 112 with a workstation 206 used by a MAC controller 208. The MAC controller 208, in one embodiment, includes an entity or automated system enabled to grant MAC access to the access candidate 108 when the grant of such access is not prohibited. To initiate access, the MAC sponsor 112 prepares an electronic access request 210 (one embodiment of the access request 114, Figure 1) using the workstation 204 and submits the electronic access request 210 to the MAC controller 208 via the network 202. In the alternative, the process may be initiated by a request for data/access by the candidate 108, which may cause MAC sponsor 112 to prepare an electronic access request 204. In preparing the electronic access request 210, the MAC sponsor 112 may utilize information provided by the access candidate 108 as a profile 212 (one embodiment of the access profile 116A, Fig. 1). The profile 212 may include one or more attributes associated with the access candidate 108, such as citizenship information, current location information, criminal record, employment information, an indication of a valid data access agreement, and the like. The profile 212 may be electronically submitted to the MAC sponsor 112 or the MAC controller 208 via the network 202 or another network connection. The profile 212 and the access profiles 116A or 116B may include the same profile. Further, in one embodiment, the access profile 116A/116B/212 is part of a graphics-based network directory available via the network 202 (described below with reference to Figure 4).

[0038] Upon receipt of the electronic access request 210, the MAC controller 208 may identify the one or more data classes associated with the portion of the secured data 102 requested by the MAC sponsor 112. The MAC controller 208 then may identify the access requirements associated with the one or more data classes and compare the access requirements with the attributes of the access candidate 108 submitted as the electronic access request 210/profile 212. In at least one embodiment, the access requirements are available to the MAC controller 208 as one or more access requirements files 214 stored on a data server of the network 202 or on the workstation 206. The access requirements file 214 preferably includes

data formatted for display as a table or other arrangement on the display of the workstation 206 (described below in Figure 5).

[0039] In deciding whether to grant access, the MAC controller 208 compares the access requirements of the identified data classes with the attributes of the access candidate 108. This comparison may be performed manually by the MAC controller 208 by, for example, visually comparing a display of the access candidate's attributes with a display of the access requirements. Alternatively, the MAC controller 208 may utilize a software application to automate the comparison. In the event that the attributes are compliant with the access requirements (i.e., the comparison indicates that access is not prohibited), the MAC controller 208 grants access to the resources 110 by, for example, providing the access candidate 108 or MAC sponsor 112 with a ID/password, changing a network profile of the access candidate 108, and the like. The MAC controller 208 further may notify the MAC sponsor 112 or access candidate 108 by sending an email or other communication via the network 202.

[0040] In the event that the attributes of the access candidate 108 are in conflict with the access requirements (i.e., the comparison indicates that access is prohibited without authorization), the MAC controller 208 may send the MAC sponsor 112 or access candidate 108 an email or other communication indicating such via the network 202. The MAC sponsor 112 and access candidate 108 then may modify the electronic access request 210 and resubmit the access request 210 or they may appeal the decision.

[0041] Referring now to Figure 3, an exemplary network-based DAC access process 300 is illustrated in accordance with at least one embodiment of the present invention. As noted above, a grant of access by the DAC security level 106 (Figure 1) preferably is required before an access candidate 108 may access the secured data 102 using the resources 110.

[0042] To initiate the DAC access process, the DAC sponsor 120 may prepare an electronic access request 302 for one or more portions of the secured data 102 on behalf of the access candidate 108 (Figure 1). As with the electronic access request 210 of Figure 2, the DAC sponsor 120 may use information obtained from the access candidate 108 in preparing the electronic access request 302. The DAC sponsor 120 then may submit the electronic access request 302 to a DAC security module 304, where the DAC security module 304 preferably is implemented as part of the network 202 (Figure 2) or similar network. The DAC security

module 304 preferably includes software and/or hardware adapted to receive the electronic access request 302 and to identify one or more DAC controllers associated with each of the one or more requested portions of the secured data 102. The DAC controllers may be identified based at least in part on the one or more data levels (e.g., application, group information or item information levels) to which the data portions are members or the data classes associated with each data portion. To illustrate, a DAC controller could be associated with each data level or a DAC controller could be associated with each data class. Alternatively, DAC controllers may be associated with various combinations of data levels and data classes. In the illustrated example, it is assumed that the electronic access request 302 requests access to data controlled by DAC controllers 306, 308.

[0043] The DAC security module 304 may be further adapted to forward the access request 302 to the applicable DAC controllers 306, 308. The access request 302 preferably is forwarded as an electronic communication received at and displayed on the workstations 310, 312 used by the DAC controllers 306, 308, respectively. The DAC controllers 306, 308 then may compare the attributes of the access candidate 108 with the access requirements 314, 316 of the corresponding data for which each DAC controller 306, 308 is responsible. Should the attributes comply with the access requirements considered by a DAC controller (i.e., access to the data controlled by a DAC controller is not prohibited), the DAC controller may provide an indication to the DAC security module 304 that access to the applicable data portion is to the DAC security module 304. The DAC security module 304 may then provide the same or similar indication to the DAC sponsor 120 or access candidate 108. The DAC security module 304, or alternatively the corresponding DAC controller, then may grant access to the requested data portion.

[0044] Should the attributes conflict with the access requirements considered by a DAC controller (i.e., access to data controlled by a DAC controller is prohibited without authorization), the DAC controller, or alternatively the DAC security module 304, may submit a resolution request 318 to the applicable resolution authority 320, where the resolution authority 320 includes an entity or automated system enabled to authorize the grant of access in such cases. As with the electronic access request 302, the resolution request 318 may be transmitted as an electronic communication to a workstation 322 used by the resolution authority 320.

[0045] The resolution authority 320 may consider the access requirements, access candidate attributes, and additional information (such as an indication of the need for access) and may request additional information in deciding whether to grant or deny, in whole or in part, authorization. After deciding whether a grant of authority is appropriate, the resolution authority 320 may transmit an indication 324 of its decision to the appropriate DAC controller. If authorized, the DAC controller may grant access to the access candidate 108 and provide an indication of such to the access candidate 108 or the DAC sponsor 120. If a grant of authority is deemed inappropriate, the DAC controller may provide an indication of such to the DAC sponsor 120 or access candidate 108.

[0046] In the event that access is granted for some but not all requested data portions, the DAC security module 304 may grant access only to the authorized portions or the security module 304 may deny access to all of the requested data portions. In the latter instance, the DAC sponsor 120 may be directed to modify the access request 302 or submit a new request so that only the authorized portions are requested.

[0047] Referring now to Figure 4, an exemplary implementation of the access profile 116A/116B/212 as an entry in an electronic directory is illustrated in accordance with at least one embodiment of the present invention. The electronic directory (not shown) may include, for example, an electronic contact information directory that is accessible, for example, via a web browser 402. To illustrate, information associated with an access candidate named "John Smith," may be displayed by the web browser 402 as a profile table 404 having a contact information portion 406, an access attributes portion 408 and a data class access portion 410. The contact information portion 406 may be used to display contact and organizational information associated with the access candidate, such as name, telephone number, email address, office location, supervisor, and the like. The access attributes portion 408 may be used to display various access attributes associated with the access candidate, such as, for example, citizenship, current location, and the existence of a valid data access agreement. In the illustrated example, the entry for access candidate "John Smith" indicates that he is a US citizen who is currently located in Paris, France and further indicating that he has signed a valid data access agreement. The data class attributes portion 410 may be used to display indications of whether the access candidate is permitted to access data associated with corresponding data classes. In

the illustrated example, the entry for the access candidate "John Smith" indicates that access by John Smith to data associated with the organizational ("ORG") data class or the special access program ("SAP") data class is not prohibited ("NP"), whereas access by John Smith to data associated with the export controlled ("EXPT") data class, the Department of Defense/Department of Energy ("DOD/DOE") data class, and the National Security Agency ("NSA") data class is prohibited without authorization ("PWA"). Of course, these data classes and levels of authorization are exemplary only and in no way limit the scope of the invention. The determination and input of an access candidate's access status (i.e., NP or PWA) for the data classes may be performed when the entry for the access candidate is formed or when each data class is considered for the first time as a result of an access request.

[0048] Referring now to Figure 5, an exemplary access requirements table 502 for display on a web browser 402 or other graphical user interface (GUI) is illustrated in accordance with at least one embodiment of the present invention. The access requirements table 502 preferably includes one or more tables illustrating the access status (i.e., not prohibited ("NP") or prohibited without authorization ("PWA")) for one or more data classes (depicted as the column headers) based on one or more access attributes (depicted as the row headers) of access candidates. To illustrate, for a U.S. citizen having a valid data access agreement and who is currently located in the U.S. or its territories, access to the NSA data class is not prohibited, whereas access to the NSA data class is prohibited without authorization for a foreign national having a valid access agreement and who is also located in the U.S. The access requirements table 502 also may include an additional requirements portion 504 indicating additional requirements in certain instances, such as, for example, a requirement that an export license be granted before access authorization is given to an access candidate who is a foreign national in the U.S. who is requesting access to the export data class.

[0049] The profile table 404 of Figure 4 and the access requirements table 502 of Figure 5 may be used by a MAC controller or DAC controller to quickly determine whether MAC access or DAC access should be granted or denied for a given access candidate. For example, a MAC controller may quickly review the information available in the access attributes portion 408 of the profile table 404 to determine whether to grant MAC access based on the correlation of the access attributes of the access candidate with the MAC access requirements. Similarly, a

DAC controller may quickly review the data class access portion 410 of the profile table 404 to determine if access to a data portion having data associated with certain data classes should be granted. In the event that the data class access portion isn't filled in or isn't available for viewing, the DAC controller may use the attributes listed in the access attributes portion 408 to identify the applicable section of the access requirements table 502 to determine if access should be granted or if authorization should be sought.

[0050] Other embodiments, uses, and advantages of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. The specification and drawings should be considered exemplary only, and the scope of the invention is accordingly intended to be limited only by the following claims and equivalents thereof.